CRYPTOME

Donate for the Cryptome archive of files from June 1996 to the present

---

20 September 2014

NSA Communications Research Centers

Previous:

NSA IDA Cryptologic Research Centers: http://cryptome.org/2013-info/09/nsa-ccr/nsa-ccr.htm

---

http://cryptome.org/2014/09/cia-crypto-restrictions.pdf

Another similar project was the creation in 1958 of the Communications Research Division (CRD) within the Institute for Defense Analysis. The CRD was a private, independent think tank dedicated to helping NSA solve advanced cryptologic problems. Co-located at Princeton University's John von Neumann Hall and a site near the Pentagon, the CRD has been led by such cryptological luminaries as Dr. [redacted] a professor of mathematics at Cornell University; [redacted] a mathematician with both the Sandia Corporation and the University of Illinois; and Dr. [redacted] the chairman of the University of Chicago's mathematics department.

http://cryptome.org/nsa-v-all.htm

Following the Baker Committee report, Killian, who was now the chairman of the board of IDA, was asked to establish a similar organization for the NSA. He agreed to do so; and following the receipt of $1.9 million in 1958, IDA's Communications Research Division was formed, and planning began for the building of offices and laboratories on Princeton's campus.

Despite the assertion of one official of the institute that IDA has always been "completely independent of the government" in order to ensure that the institute would be "able to carry out studies that don't merely support some preconceived idea of the government," the CRD has always had the most intimate ties with the NSA. Selected as CRD's first director was Dr. J. Barkley Rosser, fifty, a professor of mathematics at Cornell and a specialist in numerical analysis. Chosen as his deputy, however, was Dr. Richard A. Leibler, forty-four, a five-year employee of the Puzzle Palace and a chief architect of Project Focus. A former mathematician with the Sandia Corporation who had also taught, at various times, at the University of Illinois (where he became friends with another math professor, Dr. Louis W. Tordella), Purdue, and Princeton, Leibler was primarily interested in probability and statistics. He apparently enjoyed what he once referred to as "our lonely isolation in Princeton." In reference to NSA, he once wrote to William F. Friedman, "For reasons which you must appreciate, I try to get down there and back as soon as possible,. so I usually manage to do all my work in a single day."

On September 12, 1961, A. Adrian Albert, aged fifty-five, chairman of the University of Chicago's mathematics department, replaced Barkley Rosser as head of the CRD. One of cryptology's earliest visionaries, Albert had seen the correlation between cryptography and

higher algebra as early as 1941. In a paper entitled "Some Mathematical Aspects of Cryptography," he wrote, "It would not be an exaggeration to state that abstract cryptography is identical with abstract mathematics."

Like that of his predecessor, Albert's tenure at CRD was also short. In 1963 Deputy Director Leibler dropped the "deputy" from his title and moved into the director's office, thus tying the knot between the NSA and CRD all the tighter. The relationship must have been a good one. Leibler continued as director for the next fourteen years, leaving Princeton only in 1977 to return to the NSA as chief of the Office of Research within the Research and Engineering Organization.

Leibler was replaced by Dr. Lee P. Neuwirth, forty-three, who had served as deputy director for the previous twelve years. He had first joined CRD as a mathematician in 1961, two years after receiving his Ph.D. from Princeton.

Labeled "the most secret of the major think tanks" by Paul Dickson, in his book Think Tanks, IDA has its headquarters in a ten-story, concrete-and-glass high-rise across an acre of parking lots from the Pentagon. Eschewing even the smallest sign, IDA makes a point of not advertising its existence.

---

https://www.ida.org/IDAFFRDCs.aspx

IDA's FFRDCs

IDA operates three FFRDCs: the Systems and Analyses Center (SAC), the Center for Communications and Computing (C&C), and the Science and Technology Policy Institute (STPI). IDA operates these FFRDCs for the Office of the Secretary of Defense, the National Security Agency, and the Office of Science and Technology Policy in the Executive Office of the President and the National Science Foundation, respectively. Our sponsors turn to IDA for two very important reasons: our independence and our freedom from conflicts of interest.

IDA’s only business is to operate FFRDCs; we do no work outside the FFRDC framework. As a result, the relationship between the FFRDC and the parent corporation is very close. Unlike some FFRDCs, IDA has no other lines of business.

http://en.wikipedia.org/wiki/Institute_for_Defense_Analyses

IDA’s support of the National Security Agency began at its request in 1959, when it established the Center for Communications Research in Princeton, New Jersey. Additional requests from NSA in 1984 and 1989 led respectively to what is now called the Center for Computing Sciences in Bowie, Maryland and to a second Center for Communications Research in La Jolla, California. These groups, which conduct research in cryptology and information operations, comprise IDA’s Communications and Computing FFRDC.

Center for Communications and Computing

Since the 1950s, IDA’s Center for Communications and Computing (C&C)[14] have performed fundamental research in support of the National Security Agency’s cryptology mission in:

Foreign signals intelligence and the security of information and

Communications of the U.S. Government.

More recently, the Centers, which now consist of a Center for Computing Sciences in Bowie, Maryland, and two Centers for Communications Research with offices in Princeton, New Jersey, and La Jolla, California, have also worked on network security issues. Within those broad areas, the research portfolio particularly focuses on the creation and analysis of sophisticated encryption methods, high-speed computing technologies, the development of advanced algorithms and their applications, algorithmic and mathematical foundations of cryptology, computer network technologies supporting communications security, information processing technologies supporting cyber security, and analytical applications for large data sets. Although the Centers in Princeton and La Jolla were founded to focus on the mathematics of cryptology, and the center in Bowie was founded to focus on computational science, all three have developed distinctive areas of expertise. Nonetheless, they work closely with each other and share many overlapping research teams.

Center for Communications Research. The Communications Research Division of IDA was founded in 1959 in Princeton, New Jersey, to apply mathematical expertise to research in cryptology. In 1989 its name was changed to Center for Communications Research, and a second Center was opened in La Jolla, California.The two Centers employ more than 70 Ph.D. mathematicians and computer scientists, working on problems in cryptography, cryptanalysis, algorithms, high-performance computing, information processing, signal processing, and network security, as well as related areas of pure and applied mathematics. A surprisingly broad array of branches of the mathematical sciences have proved to be useful in this work, and this is reflected in the variety of backgrounds of the researchers at these Centers. The day-to-day work is aimed at providing practical solutions to important real-world problems faced by NSA, and this can range from deep mathematical investigations to writing advanced computer programs to sophisticated statistical analyses of data. The research environment is distinctive in encouraging close collaboration, multidisciplinary teams, tight coupling between theory and practice, and strong connections with the other Centers.

Center for Computing Sciences was founded in 1985 in Bowie, Maryland .

Center for Computing Sciences, 17100 Science Drive, Bowie, MD

CCS focuses the skills of some of the country's best computer scientists, engineers, and mathematicians on solving intelligence-related problems of importance to national security, and also on tackling problem sets of interest to the entire computational science world. CCS's original mission, the development and use of high-end computing, has expanded over the years to reflect global political and technological changes. In addition to high-performance computing for cryptography, it now includes cryptography itself, extensive projects in network security and related cyber issues, signal processing, and emerging algorithmic and mathematical techniques for analyzing extremely complex data sets. CCS works closely with National Security Agency and with US industry on the development of high-performance computing platforms - an effort that senior technology policymakers believe will require government research and development support. These platforms, aimed at meeting the specialized requirements of the most demanding national-security-related computations, will have to far exceed the capabilities of even the most sophisticated computers today. The Center is uniquely qualified to provide significant insight into this challenge, given its depth of experience in NSA's most advanced computing problems; history of sustained and vigorous dialog with many of the nation's leading high-end computer makers; and active collaborations with the united States Department of Energy's Lawrence Livermore National Laboratory, Sandia National Laboratories, and the Los Alamos National Laboratory.

https://www.ida.org/IDAFFRDCs/CenterforCommunications.aspx

Center for Communications and Computing

Lt Gen. Michael V. Hayden, USAF
Director of the National Security Agency,
breaking ground for CCR-Princeton's
new home

Since the 1950s, IDA's Center for Communications and Computing has performed fundamental research in support of the National Security Agency's mission in cryptology:

- Foreign signals intelligence and the security of information and
- Communications of the U.S. Government.

More recently, the Center for Communications and Computing – which now consists of two Centers for Communications Research with offices in Princeton, New Jersey, and La Jolla, California, and the Center for Computing Sciences in Bowie, Maryland – has also worked on network security issues.

Within those broad areas, the research portfolio focuses particularly on the creation and analysis of sophisticated encryption methods, high-speed computing technologies, the development of advanced algorithms and their applications, algorithmic and mathematical foundations of cryptology, computer network technologies supporting communications security, information processing technologies supporting cyber security, and analytical applications for large data sets.

Although the IDA Centers in Princeton and La Jolla were founded to focus on the mathematics of cryptology, and the Center in Bowie was founded to focus on computational science, all three have developed distinctive areas of expertise. Nonetheless, they work closely with each other and share many overlapping research teams.

IDA's success in providing cutting-edge research in mathematics and computer science to the National Security Agency rests on four key pillars: exceptionally talented and versatile researchers, state-of-the-art computational capabilities, a close working relationship with NSA, and ongoing engagement with the broader research community so that the work can take advantage of advances in the academic and commercial worlds.

Our People

The signals intelligence and cyber security problems the nation faces today are complex, and will require creative ideas, interdisciplinary teams, and extraordinary efforts. One of the distinctive aspects of IDA's Center for Communications and Computing is that techniques, algorithms, and software developed for one purpose can be used for diverse problems as they arise in areas outside their original sphere. The disciplinary mix at the Center for Communications and Computinggives a sense of our intellectual diversity, which is a strong force behind these serendipitous uses.

Engagement with the Broader Research Community

The research community at the Center for Communications and Computing is encouraged to maintain connections, where possible, with academic and commercial researchers. There are several opportunities for this kind of collaboration.

Perhaps the most important of these is the summer workshops, which draw academics and others to use a concerted “tiger team” approach to tackling several truly difficult problems each summer. The people invited to these workshops are diverse in many ways: they come from the academic community and other research organizations; there are many levels of experience among the attendees, who range from seasoned researchers, distinguished faculty, graduate students, even occasional undergraduates; the disciplinary backgrounds include mathematics, computer science, statistics, physics, and electrical engineering. In a typical summer, the Center for Communications and Computing hosts well more than a hundred visitors, and the intense and collegial atmosphere is well known.

Engagement with the academic community is also encouraged by inviting academics to visit to give colloquia. There are typically about 100 such talks each year, including distinguished academics from the top universities in the country.

In addition, Center for Communications and Computing researcher staff are invited to give talks at conferences, companies, and academic institutions. These range from talks at major mathematics and computer science conferences to visits to give colloquia at universities and colleges across the country (and beyond).

Finally, the Centers for Communications Research (jointly) and the Center for Computing Science each have a Visiting Committee, consisting of distinguished researchers who are invited to visit to hear about current research developments. These committees visit for three days a year, and also are asked to assess research quality, comment on outside trends, and advise IDA management.

https://www.ida.org/en/IDAFFRDCs/CenterforCommunications/Communications.aspx

Center for Communications Research

The Communications Research Division of IDA was founded in 1959 in Princeton, New Jersey, to apply mathematical expertise to research in cryptology. In 1989 its name was changed to Center for Communications Research (CCR), and a second Center was opened in La Jolla, California.

The two Centers employ more than 70 Ph.D. mathematicians and computer scientists, working on problems in cryptography, cryptanalysis, algorithms, high-performance computing, information processing, signal processing, and network security, as well as related areas of pure and applied mathematics.

A surprisingly broad array of branches of the mathematical sciences have proved to be useful in this work, which is reflected in the variety of backgrounds of the researchers at these Centers. The day-to-day work is aimed at providing practical solutions to important real-world problems faced by NSA; this can range from deep mathematical investigations to writing advanced computer programs to sophisticated statistical analyses of data. The research environment is distinctive in encouraging close collaboration, multidisciplinary teams, tight coupling between theory and practice, and strong connections with the other Centers.

http://www.idaccr.org/

Center for Communications Research - Princeton

CCR-P 2002

805 Bunn Drive
Princeton, New Jersey 08540

CCR-P is a division of The Institute for Defense Analyses in Alexandria, Virginia.

General Information

What we do
Work Status/Inclement Weather Info

CCR-P hires Ph.D. mathematicians. Find out more here.

Related Divisions

The Center for Communications Research-La Jolla (CCR-LJ) in La Jolla, California

https://www.ccrwest.org/

Center for Communications Research

La Jolla

CCR - La Jolla is a division of The Institute for Defense Analyses (IDA).

Visit our sister division at:

CCR - Princeton in Princeton, NJ

Request a covering from the La Jolla Covering Repository.

Maps and directions to CCR - La Jolla are available here.

For further information about CCR - La Jolla, contact:

Center for Communications Research
4320 Westerra Court
San Diego, California 92121-1969
Telephone: (858) 622-8600
FAX: (858) 622-8601
